EINPRESSWIRE

'Wake-Up Call' for UK Businesses as Survey Reveals Frequent Breaches Caused by Insecure Code

LONDON, UNITED KINGDOM, August 26, 2025 /EINPresswire.com/ -- SecureFlag survey of tech executives finds a majority of organisations suffered code-related security incidents, exposing an urgent need for better developer training.

A new research from SecureFlag, the leader in hands-on secure coding training, has uncovered alarming gaps in software security, with senior technology leaders reporting high rates of breaches linked to insecure code. In the survey of 100 UK C-suite and tech leaders, 67% admitted their organisation experienced at least one cybersecurity breach or serious incident in the past 12 months due to insecure coding practices. Nearly half of these companies faced multiple such incidents. Despite these dangers, the survey found that 40% of organisations still do not mandate regular secure coding training for their developers – a shortfall experts warn must be urgently addressed.

“This should be a wake-up call for every business that develops software,” said Andrea Scaduto, CEO and co-founder of SecureFlag. “It’s frankly shocking that in 2025 so many breaches are still happening because of avoidable coding flaws. Our survey exposes a clear and present danger: too many development teams lack the security training to prevent vulnerabilities, and attackers are exploiting that gap. The message is loud and clear – without a serious investment in developer education, organisations will continue to be at risk.”

The survey highlights a disconnect between awareness and action. While 88% of the executives surveyed acknowledged that poor coding practices pose a significant threat to their business, far fewer have fully implemented the safeguards to counter them. Only about one-third of companies currently provide continuous, hands-on secure coding training, and just 29% are highly confident in their developers’ ability to write code that is secure by design. Many leaders cited constraints such as limited time, budget, or available expertise as reasons for not training developers more frequently. However, the cost of inaction is steep – several respondents noted that the incidents they experienced led to customer data exposure, service downtime, and substantial financial losses.

For context, broader industry research reinforces the prevalence of the threat. According to the UK government’s Cyber Security Breaches Survey, 43% of businesses overall suffered a cyber attack or breach in the past year, underlining how common such incidents have become.

SecureFlag's findings drill down further: they implicate insecure software code as a primary culprit in many of these breaches. Common issues uncovered include developers unknowingly introducing vulnerabilities (like SQL injection and insecure authentication flows) and a lack of code review or testing rigor to catch problems before release.

Emilio Pinna, SecureFlag's CTO and co-founder, stressed the urgency of immediate action. "The fact that so many organizations are being compromised through code errors is alarming. Breaches stemming from coding mistakes are preventable – but only if companies invest in proper training," he said. "We urge businesses not to wait for a disaster. Ensuring your developers can recognize and avoid vulnerabilities must be a top priority. It's far cheaper to train a developer than to clean up after a breach."

SecureFlag is responding to this crisis by doubling down on its mission to empower development teams with the skills to build secure software from the start. Through its immersive training platform, SecureFlag helps organisations rapidly upskill their developers in real-world secure coding techniques, transforming security from an afterthought into a foundational practice. With the survey serving as a stark warning, SecureFlag calls on industry leaders to act now and join the push to eliminate insecure code – before the next breach makes headlines.

About SecureFlag:

SecureFlag is a leading provider of hands-on secure coding training and threat modeling solutions. Its platform offers interactive labs in real development environments, empowering developers, DevOps, cloud, and QA engineers to identify and remediate vulnerabilities across more than 50 technologies. SecureFlag also developed ThreatCanvas, the first AI-powered threat modeling tool that automates secure design and makes threat modeling accessible to all technical roles. Trusted by enterprises across industries, including finance, healthcare, and tech, SecureFlag helps organizations build secure software and embed security throughout the development lifecycle. Learn more at www.secureflag.com.

Lara Joseph
Eskenzi PR
+44 20 7183 2849
lara@eskenzipr.com